Math 406 Section 3.5: The Fundamental Theorem of Arithmetic

1. **Theorem (The Fundamental Theorem of Arithmetic):** Every positive integer greater than 1 can be written uniquely as a product of powers of primes Here "uniquely" means up to the order of the multiplication.

   Example: $20 = 2^2 \cdot 5$ and that's the only way. Writing $20 = 5 \cdot 2^2$ is equivalent.

   (a) **Lemma:** If $a, b, c \in \mathbb{Z}^+$ and $\gcd(a, b) = 1$ then if $a \mid bc$ then $a \mid c$
   Proof: Put $1 = \alpha a + \beta b$ then $c = c\alpha a + c\beta b$. Since $a \mid bc$ we have $a \mid c$. $\mathcal{QED}$

   (b) **Lemma:** If $p \mid a_1 ... a_n$ where p is prime, then $\exists i$ such that $p \mid a_i$.
   Proof: By induction on n. $\mathcal{QED}$

   (c) **Proof of FToA:** We prove that each positive integer greater than 1 can be written as a product of powers of primes and then we show it is unique.

   For the first part we use contradiction. Suppose there are positive integers greater than 1 which cannot be written as a product of powers of primes. Let n be the smallest such integer by well-ordering. If n is prime then we're done. If n is not prime then $n = ab$ with $1 < a < n$ and $1 < b < n$. But then a and b are products of powers of primes and so $n = ab$ is, a contradiction.

   For uniqueness suppose we have an integer $n > 1$ with two distinct factorizations into powers of primes. Expanding out the powers we have:

   $$n = p_1 p_2 ... p_i = q_1 q_2 ... q_j$$

   We can cancel any common primes so suppose we have done so to get products of distinct primes which we'll denote using the same notation in a real abuse of notation for convenience:

   $$p_1 p_2 ... p_i = q_1 q_2 ... q_j$$

   But now $p_1 \mid q_1 ... q_j$ so that p_1 divides one of the q_j, a contradiction. $\mathcal{QED}$

2. **Uses:**

   (a) **Theorem:** For $a, b \in \mathbb{Z}$ we have $a \mid b$ iff whenever p^α appears in the prime factorization of a then p^β with $\beta \geq \alpha$ appears in the prime factorization of b.
   Proof: For the backwards direction suppose we have $a = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$, then we must have $b = p_1^{\beta_1} p_2^{\beta_2} ... p_k^{\beta_k} B$ with $\beta_i \geq \alpha_i$ for each i and with B being any primes in b but not in a. Then we have:

   $$b = p_1^{\beta_1} p_2^{\beta_2} ... p_k^{\beta_k} B = a \left(p_1^{\beta_1 - \alpha_1} p_2^{\beta_2 - \alpha_1} ... p_k^{\beta_k - \alpha_1} B \right)$$

   and so $a \mid b$. For the forward direction suppose $a \mid b$. Suppose p^α appears in the prime factorization of a and p^β appears (or doesn't) in the prime factorization of b with $0 \leq \beta < \alpha$. We can write $a = p^\alpha A$ and $b = p^\beta B$ where A and B are all the other prime powers. Then we have some $c \in \mathbb{Z}$ with:

   $$\begin{aligned} ac &= b \\ p^\alpha Ac &= p^\beta B \\ p^{\alpha - \beta} Ac &= B \end{aligned}$$

   These two numbers are identical and therefore must have the same prime factorization. However there are p on the left (since $\alpha - \beta > 0$) but not on the right. This is a contradiction. $\mathcal{QED}$

(b) **Theorem:** The positive divisors of n are those integers whose prime power factorizations have the same primes as n with powers less than or equal to those powers occuring in n.
Proof: This follows from the previous theorem. $\mathcal{QED}$
Example: Suppose $n = 2^3 \cdot 5^2 \cdot 7$. Then the positive divisors of n are those integers of the form $2^a \cdot 5^b \cdot 7^c$ with $0 \leq a \leq 3$ and $0 \leq b \leq 2$ and $0 \leq c \leq 1$. Notice that there are $(4)(3)(2) = 24$ such choices and therefore 24 such factors.

(c) **Theorem:** The greatest common divisor of two integers equals the integer whose prime power factorization contains primes common to both prime power factorizations each with a power equal to the minimum power occurring in those two.
Proof: The greatest common divisor is a divisor of both and therefore the prime factorization of the gcd can contain only primes that appear in both and those primes can only appear with at most the minimum power appearing in both. The greatest common divisor will then be obtained by choosing as many primes as possible with the minimum power appearing. $\mathcal{QED}$
Example: If $a = 2^3 \cdot 7^4 \cdot 11$ and $b = 2^2 \cdot 7^5 \cdot 13^2$ then $\gcd(a, b) = 2^2 \cdot 7^4$.

(d) **Theorem:** The least common multiple of two integers equals the integer whose prime power factorization contains primes occurring in either prime power factorization each with a power equal to the maximum power occurring in those two.
Proof: The least common multiple is a multiple of both and therefore the prime factorization of the lcm must contain all the primes that appear in both and those primes must appear with at least the minimum power appearing in each. The least common multiple will then be obtained by choosing as few primes as possible with the maximum power appearing. $\mathcal{QED}$
Example: If $a = 2^3 \cdot 7^4 \cdot 11$ and $b = 2^2 \cdot 7^5 \cdot 13^2$ then $\gcd(a, b) = 2^3 \cdot 7^5 \cdot 11 \cdot 13^2$.

(e) **Theorem:** For integers a, b not both zero we have $ab = \gcd(a, b)\text{lcm}(a, b)$.
Proof: This follows from the previous two theorems since for each prime the sum of the powers equals the maximum plus the minimum. $\mathcal{QED}$

(f) **Theorem:** Suppose $n_1, n_2 \in \mathbb{Z}$ with $\gcd(n_1, n_2) = 1$. Suppose $d \mid n_1 n_2$. Then $d = d_1 d_2$ with $\gcd(d_1, d_2) = 1$ and $d_1 \mid n_1$ and $d_2 \mid n_2$.
Outline of Proof: For the first part: If a prime power p^a occurs in d then it occurs in $n_1 n_2$ to the same power or higher. Since n_1 and n_2 are relatively prime we put p^a in d_1 iff p occurs in n_1 and in d_2 iff p occurs in n_2. $\mathcal{QED}$
Note: This is not true without the relative primality. For example if $n_1 = 10$ and $n_2 = 4$ and $d = 20$ then $d \mid n_1 n_2$ but there is no way to allocate the primes in 20 into those in n_1 and those in n_2.